1118.70214 PATENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Li et al.

Serial No. 10/811,323

Conf. No. 9463

Filed: March 26, 2004

For: DIGITAL SIGNATURE GENERATION METHOD, DIGITAL SIGNATURE AUTHENTICATION METHOD, DIGITAL SIGNATURE GENERATION REQUEST PROGRAM AND DIGITAL SIGNATURE AUTHENTICATION REQUEST PROGRAM

Art Unit: 2131

Examiner: Unassigned

I hereby certify that this paper is being deposited with the United States Postal Service as FIRST-CLASS mail in an envelope addressed to: Mail Stop MISSING PARTS, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this date.

August 9, 2004
Date

Registration No. 29,367

F-CLASS.WCM
Appr. February 20, 1998

Attorney for Applicant

CLAIM FOR PRIORITY

Mail Stop MISSING PARTS
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Applicants claim foreign priority benefits under 35 U.S.C. § 119 on the basis of the foreign application identified below:

Japanese Patent Application No. 2003-092280, filed March 28, 2003.

A certified copy of the priority document is enclosed.

Respectfully submitted,

GREER, BURNS & CRAIN, LTD.

By

Patrick G. Burns
Registration No. 29,367

Customer No. 24978

August 9, 2004
300 South Wacker Drive
Suite 2500
Chicago, Illinois 60606
Tel: (312) 360-0080
Fax: (312) 360-9315
P:\DOCS\1118\70214\628580.DOC

日本国特許庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日
Date of Application: ２００３年　３月２８日

出願番号
Application Number: 特願２００３－０９２２８０

[ST. 10/C]: [ＪＰ２００３－０９２２８０]

出願人
Applicant(s): 富士通株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

２００３年１２月　８日

特許庁長官
Commissioner,
Japan Patent Office

今井康夫

出証番号　出証特２００３－３１０１３

【書類名】　特許願

【整理番号】　0252392

【あて先】　特許庁長官　殿

【国際特許分類】　G09C　1/00　640

【発明の名称】　電子署名生成方法，電子署名検証方法，電子署名生成依頼プログラム，及び電子署名検証依頼プログラム

【請求項の数】　4

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　李　濤

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　小泉　潤一

【発明者】

【住所又は居所】　神奈川県川崎市中原区上小田中４丁目１番１号　富士通株式会社内

【氏名】　加藤　広己

【発明者】

【住所又は居所】　神奈川県横浜市港北区新横浜二丁目４番地１９　株式会社富士通ハイパーソフトテクノロジ内

【氏名】　宮崎　達弘

【特許出願人】

【識別番号】　000005223

【氏名又は名称】　富士通株式会社

【代理人】

【識別番号】　100098235

【弁理士】

【氏名又は名称】　金井　英幸

【手数料の表示】

【予納台帳番号】　062606

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9908696

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　電子署名生成方法，電子署名検証方法，電子署名生成依頼プログラム，及び電子署名検証依頼プログラム

【特許請求の範囲】

【請求項１】

ネットワークを介して端末とサーバ装置とが通信可能に構成されているシステム上において、前記端末の記憶部内に存在している電子情報に対する電子署名を生成するための電子署名生成方法であって、

前記端末が、前記電子情報のダイジェスト値を算出し、

前記端末が、前記ダイジェスト値，及び、前記電子情報の発行元が有する識別情報を、前記サーバ装置へ送信し、

前記サーバ装置が、予め各識別情報毎に秘密鍵及び公開鍵を対応付けて格納している記憶装置から、前記端末から受信した識別情報に対応する秘密鍵を取り出し、

前記サーバ装置が、前記端末から受信したダイジェスト値を前記記憶装置から取り出した秘密鍵によって暗号化することによって署名値を生成し、

前記サーバ装置が、生成した署名値を前記端末へ応答し、

前記端末が、前記サーバ装置から応答された署名値及び前記識別情報を前記電子情報に添付することによって電子署名付き電子情報を構成する

ことを特徴とする電子署名生成方法。

【請求項２】

ネットワークを介して端末とサーバ装置とが通信可能に構成されているシステム上において、請求項１記載の電子署名生成方法によって得られた電子署名付き電子情報を検証するための電子署名検証方法であって、

前記端末が、前記電子署名付き電子情報中の電子情報のダイジェスト値を算出し、

前記端末が、前記ダイジェスト値，並びに、前記電子署名付き電子情報中の前記署名値及び前記識別情報を、前記サーバ装置へ送信し、

前記サーバ装置が、前記端末から受信した識別情報に対応する公開鍵を前記記

憶装置から取り出し、

前記サーバ装置が、前記端末から受信した署名値を前記記憶装置から取り出した公開鍵によって復号化し、

前記サーバ装置が、復号化した前記署名値の内容と前記端末から受信したダイジェスト値とが一致しているか否かを比較し、

前記サーバ装置が、前記比較の結果を前記端末へ応答する

ことを特徴とする電子署名検証方法。

【請求項３】

予め各識別情報毎に秘密鍵及び公開鍵を対応付けて記憶する記憶装置を有するとともに、暗号化対象情報及び識別情報を指定した電子署名生成依頼メッセージを受信した時には、受信した識別情報に対応する秘密鍵を前記記憶装置から取り出し、取り出した秘密鍵によって前記暗号化対象情報を暗号化することによって署名値を生成し、生成した署名値を応答するサーバ装置との間で、ネットワークを通じて通信可能なコンピュータに対して、

電子情報及び当該電子情報の発行元の識別情報が入力された場合には、

前記電子情報のダイジェスト値を算出させ、

算出されたダイジェスト値を前記暗号化対象情報として前記識別情報とともに指定した電子署名生成依頼メッセージを、前記サーバ装置へ送信させ、

前記サーバ装置から前記署名値が応答された場合には、

当該署名値及び前記識別情報を前記電子情報に添付することによって電子署名付き電子情報を構成させる

ことを特徴とする電子署名生成依頼プログラム。

【請求項４】

予め各識別情報毎に秘密鍵及び公開鍵を対応付けて記憶する記憶装置を有するとともに、検証対象情報，署名値及び識別情報を指定した電子署名検証依頼メッセージを受信した時には、受信した識別情報に対応する公開鍵を前記記憶装置から取り出し、取り出した公開鍵によって前記署名値を復号化し、復号化された署名値と前記検証対象情報とが一致しているか否かを比較して、比較結果を応答するサーバ装置との間で、ネットワークを通じて通信可能なコンピュータに対して

、

前記請求項１又は３に従って得られた電子署名付き電子情報が入力された場合には、

前記電子署名付き電子情報中の電子情報のダイジェスト値を算出させ、

当該ダイジェスト値を前記検証対象情報として前記電子署名付き電子情報中の前記署名値及び前記識別情報とともに指定した電子署名検証依頼メッセージを、前記サーバ装置へ送信させる

ことを特徴とする電子署名検証依頼プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、ネットワークを介して複数の利用者端末とサーバ装置とが通信可能に構成されているシステム上において、何れかの利用者端末内に存在している電子情報に対する電子署名を生成するための電子署名生成方法，このような電子署名生成方法に従って生成された電子署名を検証するための電子署名検証方法，電子署名生成機能を有するサーバ装置と通信可能なコンピュータに上記電子署名生成方法を実施させる電子署名生成依頼プログラム，及び、電子署名検証機能を有するサーバ装置と通信可能なコンピュータに上記電子署名検証方法を実施させる電子署名検証依頼プログラムに、関する。

【０００２】

【従来の技術】

従来、電子情報の暗号化及び電子署名の方法として、ＲＳＡ公開鍵方式が知られている。このＲＳＡ公開鍵方式とは、一方の鍵を用いて暗号化された電子情報は他方の鍵を用いなければ復号化できないという関係にある鍵ペアを生成し、そのうちの一つを秘密鍵として非公開とするとともに、他の一つを公開鍵として第三者に公開する方式である。そして、電子署名をする際には、署名対象電子情報をその発行者固有の秘密鍵によって暗号化して電子署名を生成し、この電子署名を暗号化前の署名対象電子情報（以下、「平文の署名対象電子情報」という）に添付して、当該電子情報の相手方へ渡す。この電子署名付きの電子情報を受け取

った相手方は、その電子情報の発行者のものとして公開されている公開鍵を用いて電子署名を復号化し、復号化によって再現された電子情報と平文の電子情報とを照合し、両者が一致していれば、その平文の電子情報が真正なものであると判断することができ、両者が一致していなければ、その平文の電子情報が真正なものではない（即ち、表示された発行者以外の者によって偽造されたか、第３者によって改竄されたものである）と判断することができる。

【０００３】

【特許文献１】　特開２００２－３３７６０号公報

【０００４】

以上のような電子署名の生成及び電子署名の検証は、電子情報を発行する者及び電子情報を受け取った者が自らが管理する端末上で行うのが基本であるが、ネットワークを通じてこれらの者から電子署名の作成及び検証の依頼を受けてこれらの作業を代行するサービスも、実施されている。このような代行サービスを行うサービス提供者が運営するサーバ装置は、契約を取り交わした各利用者の鍵ペアを予め登録しておき、何れかの利用者が操作する端末から電子署名作成依頼及び署名対象電子情報をネットワーク経由で受け取ると、その利用者の秘密鍵によって当該署名対象電子情報を暗号化して電子署名を生成し、生成した電子署名を依頼元利用者が操作する端末へ返送する。依頼元利用者は、サーバ装置から受け取った電子署名を平文の署名対象電子情報に添付して、当該電子情報の相手方へ渡す。この電子署名付きの電子情報を受け取った相手方は、これら平文の電子情報及び電子署名をネットワーク経由で自ら操作する端末からサーバ装置へ送信し、電子署名の検証を依頼する。検証依頼を受けたサーバ装置は、その電子署名の発行者のものとして登録されている公開鍵によって電子署名を復号化し、復号化によって再現された電子情報と平文の電子情報とを照合し、両者が一致していれば、その平文の電子情報が真正なものである旨を依頼者操作の端末へ応答し、両者が一致していなければ、その平文の電子情報が真正なものではない旨を依頼者操作の端末へ応答する。

【０００５】

【発明が解決しようとする課題】

しかしながら、従来の電子署名生成方法及び電子署名検証方法によると、各個人が管理する端末上において電子署名の生成又は検証を行う場合であっても、電子情報の発行者又は相手方から依頼を受けたサーバ装置上において電子署名の生成又は検証を行う場合であっても、夫々、以下のような問題がある。

【０００６】

すなわち、各個人が管理する端末上において電子署名の生成及び検証を行う場合には、その個人は、自己の鍵ペア，特に秘密鍵を、紛失することが無い様、また、他人に漏洩してしまうことが無い様、維持及び管理しなければならず、また、自ら電子署名の作成及び検証をしなければならない。そのため、その個人は、鍵の生成，維持管理，電子署名の作成，電子署名の検証を行うためのソフトウェアを、端末のハードウェアに加えて、導入しなければならない。よって、その個人は、これらソフトウェア及びハードウェアの導入及び維持コストや運用管理コストを負担しなければならないのみならず、運用ノウハウを自ら蓄積するか他者から提供されなければならない。

【０００７】

また、ネットワーク上のサーバ装置上において電子署名の生成及び検証を行う場合には、電子署名の作成を依頼する利用者は、平文の電子情報をネットワーク経由でサーバ装置へ送らねばならない。また、電子署名の検証を依頼する利用者は、電子署名に添付して平文の電子情報をネットワーク経由でサーバ装置へ送らねばならない。これら利用者が操作する端末とサーバ装置との間においては、実装の普及しているＳＳＬ（Secure Socket Layer）を使用すれば、第三者による不正アクセスは或る程度防止することができる（また、電子署名を添付した電子情報を発行者と相手方との間で交換する間も、ＲＳＡ公開鍵暗号化アルゴリズム等の暗号化技術を利用することによって第三者による不正アクセスを防止することができる）。しかしながら、サーバ装置内においては、暗号化前又は復号化後の電子情報は平文であるので、このサーバ装置を運営するサービス提供者に対して電子情報の内容を隠すことができない。

【０００８】

本発明は、以上のような問題点に鑑みてなされたものであり、電子署名の作成

又は検証をネットワーク上のサーバ装置上において代行することによって各個人の負担を軽減することができるとともに、署名対象電子情報そのものをサーバ装置において暗号化又は復号化することなく電子署名として機能する暗号化情報を作成し、また、署名対象電子情報の検証を行うことができる電子署名作成方法及び電子署名検証方法，電子署名生成機能を有するサーバ装置と通信可能なコンピュータに上記電子署名生成方法を実施させる電子署名生成依頼プログラム，並びに、電子署名検証機能を有するサーバ装置と通信可能なコンピュータに上記電子署名検証方法を実施させる電子署名検証依頼プログラムの提供を、課題とする。

【０００９】

【課題を解決するための手段】

上記課題を解決するために案出された本発明による電子署名生成方法によると、署名対象電子情報の発行元が操作する発行元端末は、署名対象電子情報のダイジェスト値を算出し、このダイジェスト値，及び、署名対象電子情報の発行元が有する識別情報を、サーバ装置へ送信する。すると、サーバ装置は、予め各識別情報毎に秘密鍵及び公開鍵を対応付けて格納している記憶装置から、発行元端末から受信した識別情報に対応する秘密鍵を取り出し、発行元端末から受信したダイジェスト値を記憶装置から取り出した秘密鍵によって暗号化することによって署名値を生成し、生成した署名値を発行元端末へ応答する。すると、発行元端末は、サーバ装置から応答された署名値及び識別情報を署名対象電子情報に添付することによって、電子署名付き電子情報を構成する。

【００１０】

また、上記課題を解決するために案出された本発明による電子署名検証方法によると、発行元から電子署名付き電子情報を受け取った相手方が操作する相手方端末は、この電子署名付き電子情報中の電子情報のダイジェスト値を算出し、このダイジェスト値，並びに、前記電子署名付き電子情報中の署名値及び識別情報をサーバ装置へ送信し、相手方端末から受信した識別情報に対応する公開鍵を記憶装置から取り出し、相手方端末から受信した署名値を前記記憶装置から取り出した公開鍵によって復号化し、復号化した署名値の内容と相手方端末から受信したダイジェスト値とが一致しているか否かを比較し、比較の結果を相手方端末へ

応答する。

【００１１】

このように構成される本発明による電子署名生成方法及び電子署名検証方法によれば、電子署名の実体である署名値は、署名対象電子情報そのものではなく、発行元端末内において署名対象電子情報に基づいて算出されたダイジェスト値をサーバ装置内において暗号化することによって生成された値である。従って、本発明によれば、電子署名の生成及び検証をネットワーク上のサーバ装置上において代行することによって利用者の負担を軽減することができるにも拘わらず、電子署名の作成時においても検証時においても、署名対象電子情報そのものはサーバ装置内に存在しないので、その内容がサーバ装置の管理運営者に知られることがない。

【００１２】

なお、本発明による電子署名生成依頼プログラムは、上記発行元端末としてのコンピュータに対して、電子情報及び当該電子情報の発行元の識別情報が入力された場合には、前記電子情報のダイジェスト値を算出させ、算出されたダイジェスト値を前記暗号化対象情報として前記識別情報とともに指定した電子署名生成依頼メッセージを、前記サーバ装置へ送信させ、前記サーバ装置から前記署名値が応答された場合には、当該署名値及び前記識別情報を前記電子情報に添付することによって電子署名付き電子情報を構成させるプログラムである。

【００１３】

また、本発明による電子署名検証依頼プログラムは、上記相手方端末としてのコンピュータに対して、上記電子署名付き電子情報が入力された場合には、前記電子署名付き電子情報中の電子情報のダイジェスト値を算出させ、当該ダイジェスト値を前記検証対象情報として前記電子署名付き電子情報中の前記署名値及び前記識別情報とともに指定した電子署名検証依頼メッセージを、前記サーバ装置へ送信させるプログラムである。

【００１４】

【発明の実施の形態】

以下、図面に基づいて、本発明の実施の形態を説明する。本実施形態における

署名対象電子情報はＸＭＬ文書であるので、以下、「署名対象コンテンツ」と称する。

【００１５】

図１は、本発明による電子署名生成方法及び電子署名検証方法を実施するための電子署名システムの概略構成を示すブロック図である。この電子署名システムは、電子署名代行サービス業者が管理運営する一台のサーバ装置（認証センターサーバ装置）１と、この電子署名代行サービス業者と電子署名代行についての契約を取り交わしている複数の利用者が夫々使用する複数の利用者端末２（図１においては１台のみ図示）とが、ネットワークＮを介して互いに通信可能に接続されることにより、構成されている。なお、このネットワークＮとしては、例えば、インターネットが利用可能であり、その場合には、認証センターサーバ装置１と各利用者端末２との間の通信は、ＨＴＴＰ（Hyper Text Transfer Protocol）に従ってなされる。

【００１６】

認証センターサーバ装置１は、ネットワークサーバ機能を有するコンピュータであり、そのハードウェアは、装置全体を制御するＣＰＵ（Central Processing Unit）１０と、このＣＰＵ１０に対してバスＢを介して接続された通信部１１，ＲＡＭ（Random Access Memory）１２及びＨＤＤ（Hard Disk Drive）１３とから、構成されている。このうち、通信部１１は、ＨＤＤ１３に格納されてＣＰＵ１０によって実行されるプログラム（デバイスドライバ）によって制御され、ネットワークＮとのインターフェースをなす通信アダプタである。また、ＲＡＭ１２は、ＣＰＵ１０によって用いられる作業領域が展開される主記憶装置である。

【００１７】

また、ＨＤＤ１３は、各種プログラム及び各種データを格納する記憶装置としてのコンピュータ可読媒体である。このＨＤＤ１３が格納する各種プログラムには、上述したデバイスドライバや通信機能を有する基本プログラムであるＯＳ（Operation System）の他、後においてフローチャートを用いて説明する電子署名代行プログラムが含まれている。この電子署名代行プログラムは、ＣＰＵ１０に

対して、各利用者端末２から送信されてきた電子署名代行依頼（署名対象コンテンツ及び当該利用者端末２を使用する利用者固有の鍵ＩＤを含む）に応じて電子署名生成を行わせ、また、各利用者端末２から送信されてきた電子署名検証依頼（署名対象コンテンツ，電子署名の実体である署名値及び当該利用者端末２を使用する利用者固有の鍵ＩＤを含む）に応じて電子署名検証を行わせるプログラムであり、ＲＡＭ１２上に読み出される署名生成部１２１，署名検証部１２２及び鍵管理部１２３の各モジュールから、構成されている。署名生成部１２１は、電子署名生成を行うモジュールであり、署名検証部１２２は、電子署名検証を行うモジュールであり、鍵管理部１２３は、署名生成部１２１又は署名検証部１２２によって呼び出されて指定された利用者の秘密鍵又は公開鍵を検索するモジュールである。

【００１８】

また、ＨＤＤ１３が格納する各種データには、各利用者について予め生成された鍵ペア（秘密鍵及び公開鍵）を格納するためのテーブルである鍵格納庫１３１が含まれている。この鍵格納庫１３１は、具体的には図２に示すデータ構造を有しており、各利用者毎に、その利用者に対して予め通知されている識別情報（鍵ＩＤ）及びパスワード（ＰＷ）の組，並びに、秘密鍵及び公開鍵を１レコードに登録することにより、構成されている。

【００１９】

一方、各利用者端末２は、ネットワークアクセス機能を有する一般的なパーソナルコンピュータであり、そのハードウェアは、装置全体を制御するＣＰＵ（Central Processing Unit）２０と、このＣＰＵ２０に対してバスＢを介して接続された通信部２１，ＲＡＭ２２，ＨＤＤ２３，ディスプレイ２４及び入力装置２５とから、構成されている。このうち、通信部２１は、ＨＤＤ２３に格納されてＣＰＵ２０によって実行されるプログラム（デバイスドライバ）によって制御され、ネットワークＮとのインターフェースをなす通信アダプタである。また、ＲＡＭ２２は、ＣＰＵ２０によって用いられる作業領域が展開される主記憶装置である。また、入力装置２５は、利用者に属する担当者によって操作されることによって、ＣＰＵ２０に各種情報を入力するキーボード，ポインティングデバイス

等である。また、ディスプレイ２４は、ＣＰＵ１０によって生成された各種画面を表示するための表示装置である。

【００２０】

また、ＨＤＤ２３は、各種プログラム及び各種データを格納するコンピュータ可読媒体である。このＨＤＤ２３が格納する各種プログラムには、上述したデバイスドライバや通信機能を有する基本プログラムであるＯＳ（Operation System）の他、署名対象コンテンツを生成するアプリケーションプログラムや、後においてフローチャートを用いて説明する電子署名依頼プログラムが含まれている。この電子署名依頼プログラムは、ＣＰＵ２０に対して、アプリケーションプログラムが記憶部としてのＲＡＭ２２上で生成した署名対象コンテンツ又は記憶部としてのＲＡＭ２２上に取り込まれた署名対象コンテンツに対する電子署名代行依頼を認証センターサーバ装置１へ送信させ、また、通信部２１又は図示せぬリムーバブル記憶媒体からＲＡＭ２２上に取り込まれた電子署名付きコンテンツの検証依頼を認証センターサーバ装置１へ送信させるプログラムであり、ＲＡＭ２２上に読み出されるコンテンツ構成部２２１及びDigest値計算部２２２の各モジュールを、含んでいる。コンテンツ構成部２２１は、認証センターサーバ装置１に対して電子署名作成依頼を行ってその結果として応答された署名値（電子署名）に署名対象電子情報及び鍵ＩＤを添付してＸＭＬ（Extended Markup Language）ファイル形式の電子署名付きコンテンツ（電子情報）として構成するとともに、認証センターサーバ装置１に対して電子署名検証依頼を行ってその結果として応答される検証結果をディスプレイ２４に表示させるモジュールである。Digest値計算部２２２は、コンテンツ構成部２２１によって呼び出され、指定された署名対象コンテンツ（ＸＭＬ文書）のDigest値（ハッシュ値）を算出するモジュールである。

【００２１】

以下、上述した利用者端末１上での電子署名依頼プログラムによる処理及び認証センターサーバ装置２上での電子署名代行プログラムによる処理を、電子署名生成時及び電子署名検証時に分けて、夫々説明する。

【００２２】

まず、署名対象コンテンツ発行元のユーザ端末２と認証センターサーバ装置１との間において電子署名生成時に実行される電子署名依頼プログラム及び電子署名代行プログラムによる処理を、図３のフローチャート（電子署名依頼プログラム），図４のフローチャート（電子署名代行プログラム）及び図５のシーケンス図を参照して説明する。

【００２３】

操作者が入力装置２５を操作することによって所定のコマンドを入力すると、ユーザ端末２において、図３に示す電子署名依頼プログラムがスタートする。なお、このコマンドには、署名対象コンテンツのパス，鍵ＩＤ及びパスワードが、パラメータとして含まれている。

【００２４】

スタート後最初のＳ０１において、電子署名依頼プログラムは、コマンドにてパラメータとして指定された鍵ＩＤ及びパスワードとともに、指定されたパスが示す署名対象コンテンツを取り込む。

【００２５】

次のＳ０２では、電子署名依頼プログラムは、Digest値計算部２２２を起動して、Ｓ０１にて取り込んだ署名対象コンテンツのDigest値の算出を命じる。

【００２６】

次のＳ０３では、電子署名依頼プログラムは、Ｓ０１にて取込んだ鍵ＩＤ及びパスワードとDigest値計算部２２２によって算出されたDigest値とを含む電子署名生成依頼メッセージを、通信部２１を経由して認証センターサーバ装置１へ送信する。その後、電子署名依頼プログラムは、Ｓ０４において、Ｓ０３にて送信した電子署名生成依頼メッセージに対する応答（即ち、後述する署名値）を認証センターサーバ装置１から受信するのを待つ。

【００２７】

認証センターサーバ装置１内においては、この電子署名作成依頼メッセージを受信すると、図４に示す電子署名代行プログラムがスタートする。スタート後最初のＳ１１では、署名作成部１２１が、鍵管理部１２３を起動して、利用者端末２から受信した電子署名生成依頼メッセージに含まれる鍵ＩＤ及びパスワードの

組合せに対応する秘密鍵を、鍵格納庫１３１から検索させる。鍵管理部１２３は、そのような秘密鍵が鍵格納庫１３１内に存在する場合にはその秘密鍵を署名生成部１２１に応答するが、そのような秘密鍵が存在しない場合（鍵ＩＤとパスワードとが対応していない場合も含む）には、依頼元利用者端末２に対してエラーメッセージを送信する。

【００２８】

秘密鍵を受け取った署名生成部１２１は、次のＳ１２において、利用者端末２から受信した電子署名生成依頼メッセージに含まれるDigest値を、鍵管理部１２３から受け取った秘密鍵によって暗号化することにより、電子署名の実体である「署名値」を生成する。

【００２９】

次のＳ１３では、署名生成部１２１は、Ｓ１２にて生成した「署名値」を、通信部１１を経由して依頼元利用者端末２へ送信する。

【００３０】

依頼元利用者端末２内においては、電子署名依頼プログラムは、認証センターサーバ装置１から「署名値」を受信すると、処理をＳ０４からＳ０５へ進める。

【００３１】

Ｓ０５では、電子署名依頼プログラムは、コンテンツ構成部２２１を起動して、Ｓ０１にて取り込んだ署名対象コンテンツに、同じくＳ０１にて取り込んだ鍵ＩＤ及びＳ０４にて認証センターサーバ装置１から受信した「署名値」を添付して、その全体をＸＭＬファイルに格納することによって、電子署名付きコンテンツを構成する。このようにして構成された電子署名付きコンテンツは、必要に応じて暗号化され、電子メールに格納された状態でネットワークＮを通じて、若しくは、リムーバブル媒体に格納された状態で、その相手方へ送られる。

【００３２】

次に、コンテンツの相手方のユーザ端末２と認証センターサーバ装置１との間において電子署名検証時に実行される電子署名依頼プログラム及び電子署名代行プログラムによる処理を、図６のフローチャート（電子署名依頼プログラム），図７のフローチャート（電子署名代行プログラム）及び図８のシーケンス図を参

照して説明する。

【００３３】

操作者が入力装置２５を操作することによって所定のコマンドを入力すると、ユーザ端末２において、図６に示す電子署名依頼プログラムがスタートする。なお、このコマンドには、電子署名付きコンテンツのパスが、パラメータとして含まれている。

【００３４】

スタート後最初のＳ２１において、電子署名依頼プログラムは、コマンドにてパラメータとして指定されたパスが示す電子署名付きコンテンツを取り込む。

【００３５】

次のＳ２２では、電子署名依頼プログラムは、コンテンツ構成部２２１を起動して、Ｓ２１にて取り込んだ電子署名付きコンテンツから、署名対象コンテンツ，「署名値」及び鍵ＩＤを、夫々抽出する。

【００３６】

次のＳ２３では、電子署名依頼プログラムは、Digest値計算部２２２を起動して、Ｓ２２にて抽出した署名対象コンテンツのDigest値の算出を命じる。

【００３７】

次のＳ２４では、電子署名依頼プログラムは、Ｓ２２にて抽出した鍵ＩＤ及び「署名値」とDigest値計算部２２２によって算出されたDigest値とを含む電子署名検証依頼メッセージを、通信部２１を経由して認証センターサーバ装置１へ送信する。その後、電子署名依頼プログラムは、Ｓ２５において、Ｓ２４にて送信した電子署名検証依頼メッセージに対する応答（即ち、後述する検証結果）を認証センターサーバ装置１から受信するのを待つ。

【００３８】

認証センターサーバ装置１内においては、この電子署名検証依頼メッセージを受信すると、図７に示す電子署名代行プログラムがスタートする。スタート後最初のＳ３１では、署名検証部１２２が、鍵管理部１２３を起動して、利用者端末２から受信した電子署名検証依頼メッセージに含まれる鍵ＩＤに対応する公開鍵を、鍵格納庫１３１から検索させる。鍵管理部１２３は、そのような公開鍵が鍵

格納庫１３１内に存在する場合にはその公開鍵を署名検証部１２２に応答するが、そのような公開鍵が存在しない場合には、依頼元利用者端末２に対してエラーメッセージを送信する。

【００３９】

公開鍵を受け取った署名検証部１２２は、次のＳ３２において、利用者端末２から受信した電子署名検証依頼メッセージに含まれる「署名値」を、鍵管理部１２３から受け取った公開鍵によって復号化する。

【００４０】

次のＳ３３では、署名検証部１２２は、Ｓ３２にて復号化した「署名値」の内容が、利用者端末２から受信した電子署名検証依頼メッセージに含まれるDigest値と一致するか否かを、チェックする。

【００４１】

そして、両者が一致している場合は、Digest値算出の元となった署名対象コンテンツが、その発行元によって電子署名依頼されたコンテンツ（即ち、その発行元の秘密鍵によって暗号化されたDigest値を算出する元となったコンテンツ）そのものであることが明らかであるので、署名検証部１２２は、Ｓ３４において、署名検証結果：ＯＫを、通信部１１を経由して依頼元利用者端末２へ送信する。

【００４２】

これに対して、両者が一致しなかった場合は、Digest値算出の元となった署名対象コンテンツが、その発行元によって電子署名依頼されたコンテンツ（即ち、その発行元の秘密鍵によって暗号化されたDigest値を算出する元となったコンテンツ）そのものである保証がない（即ち、発行元の秘密鍵によってDigest値が暗号化されてはいるが元々別のコンテンツである可能性がある，若しくは、発行元以外の者の秘密鍵によってそのコンテンツのDigest値が暗号化された可能性がある）ので、署名検証部１２２は、Ｓ３５において、署名検証結果：ＮＧを、通信部１１を経由して依頼元利用者端末２へ送信する。

【００４３】

依頼元利用者端末２内においては、電子署名依頼プログラムは、認証センターサーバ装置１から何れかの署名検証結果を受信すると、処理をＳ２５からＳ２６

へ進め、その署名検証結果をディスプレイ２４上に表示する。

【００４４】

以上説明したように、本実施形態の電子署名システムは、電子署名の生成及び検証が各利用者端末２からネットワークＮを介して認証センターサーバ装置１に代行依頼される方式を採用するにも拘わらず、認証センターサーバ装置１内において実際に利用者の秘密鍵によって「署名値」として暗号化される情報（従って、認証センターサーバ装置１内において利用者の公開鍵によって「署名値」から復元される情報）は、署名対象コンテンツそのものではなく、その署名対象コンテンツから算出されたDigest値（ハッシュ値）でしかない。このDigest値は一つのコンテンツから一意に生成されるが、そのDigest値に基づいて元のコンテンツの内容を再現することはできない。従って、このDigest値を受け取り、また、Digest値を復元した認証センターサーバ装置１は、署名対象コンテンツの内容を知ることはできないが、間接的に、発行元によって電子署名作成依頼された署名対象コンテンツと相手方によって電子署名検証依頼された署名対象コンテンツとの異同を検証することができる。

【００４５】

【発明の効果】

以上のように構成された本発明によると、電子署名の作成又は検証をネットワーク上のサーバ装置上において代行可能とすることによって、各個人の負担を軽減することができると同時に、署名対象電子情報そのものをサーバ装置において暗号化又は復号化することなく、電子署名として機能する署名値を作成することができるので、署名対象電子情報の内容がサーバ装置の運営者に知られることはない。

【図面の簡単な説明】

【図１】　本発明の実施の形態である電子署名システムのブロック図

【図２】　鍵格納庫のデータ構成を論理的に示す表

【図３】　電子署名生成時における電子署名依頼プログラムによる利用者端末内での処理内容を示すフローチャート

【図４】　電子署名生成時における電子署名代行プログラムによる認証センター

サーバ装置内での処理内容を示すフローチャート

【図５】　電子署名生成時における情報の流れを示すシーケンス図

【図６】　電子署名検証時における電子署名依頼プログラムによる利用者端末内での処理内容を示すフローチャート

【図７】　電子署名検証時における電子署名代行プログラムによる認証センターサーバ装置内での処理内容を示すフローチャート

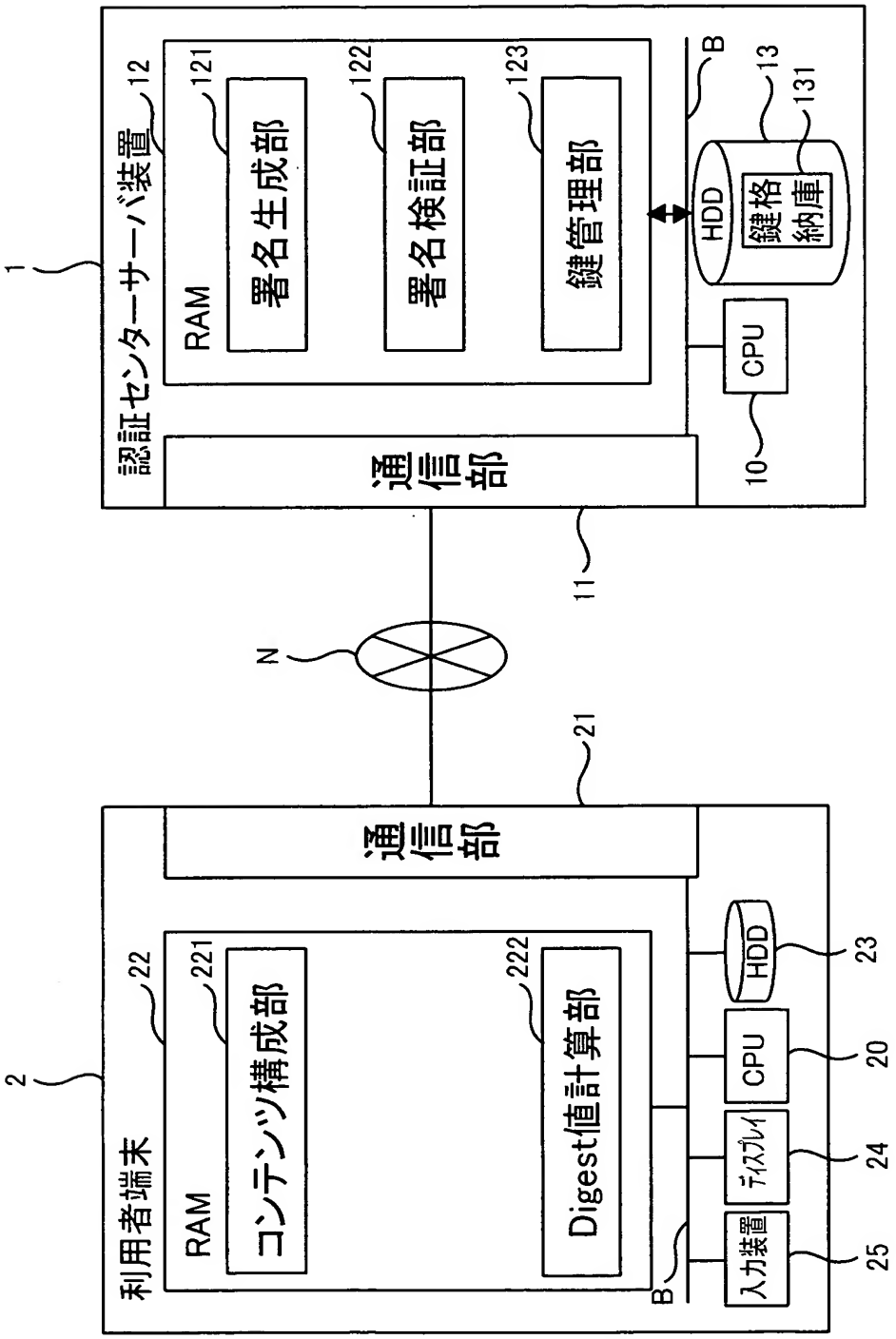
【図８】　電子署名検証時における情報の流れを示すシーケンス図

【符号の説明】

１	認証センターサーバ装置
２	利用者端末
１０	ＣＰＵ
１１	通信部
１２	ＲＡＭ
１３	ＨＤＤ
２０	ＣＰＵ
２１	通信部
２２	ＲＡＭ
２３	ＨＤＤ
２４	ディスプレイ
２５	入力装置
１２１	署名生成部
１２２	署名検証部
１２３	鍵管理部
１３１	鍵格納庫
２２１	コンテンツ構成部
２２２	Digest値計算部

【書類名】　図面

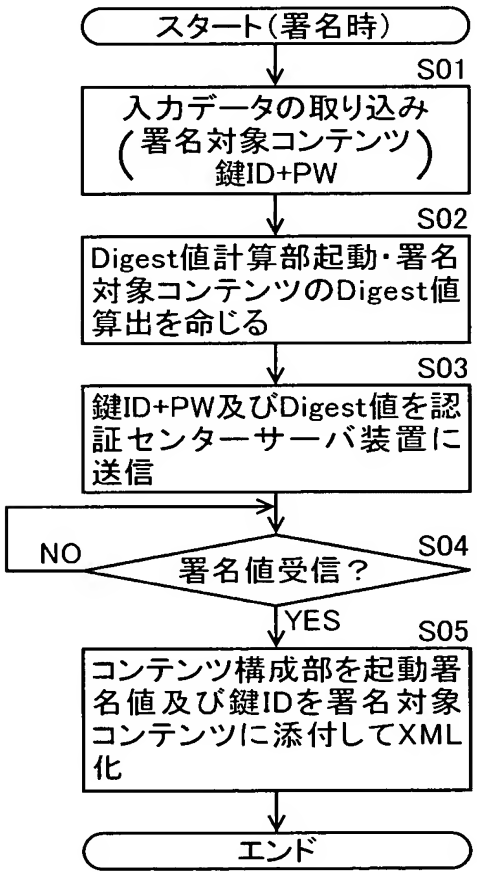
【図１】


認証センターサーバ装置
12
RAM
121
署名生成部
122
署名検証部
123
鍵管理部
B
13
131
HDD
鍵格納庫
CPU
10
通信部
11
1
N
21
通信部
利用者端末
22
RAM
221
コンテンツ構成部
222
Digest値計算部
B
HDD
23
CPU
20
ディスプレイ
24
入力装置
25
2

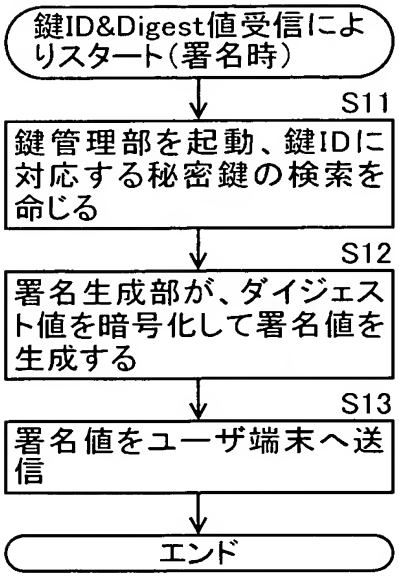
【図２】

利用者A	鍵ID-A	PW-A	秘密鍵A	公開鍵A
利用者B	鍵ID-B	PW-B	秘密鍵B	公開鍵B
利用者C	鍵ID-C	PW-C	秘密鍵C	公開鍵C
利用者D	鍵ID-D	PW-D	秘密鍵D	公開鍵D
利用者E	鍵ID-E	PW-E	秘密鍵E	公開鍵E

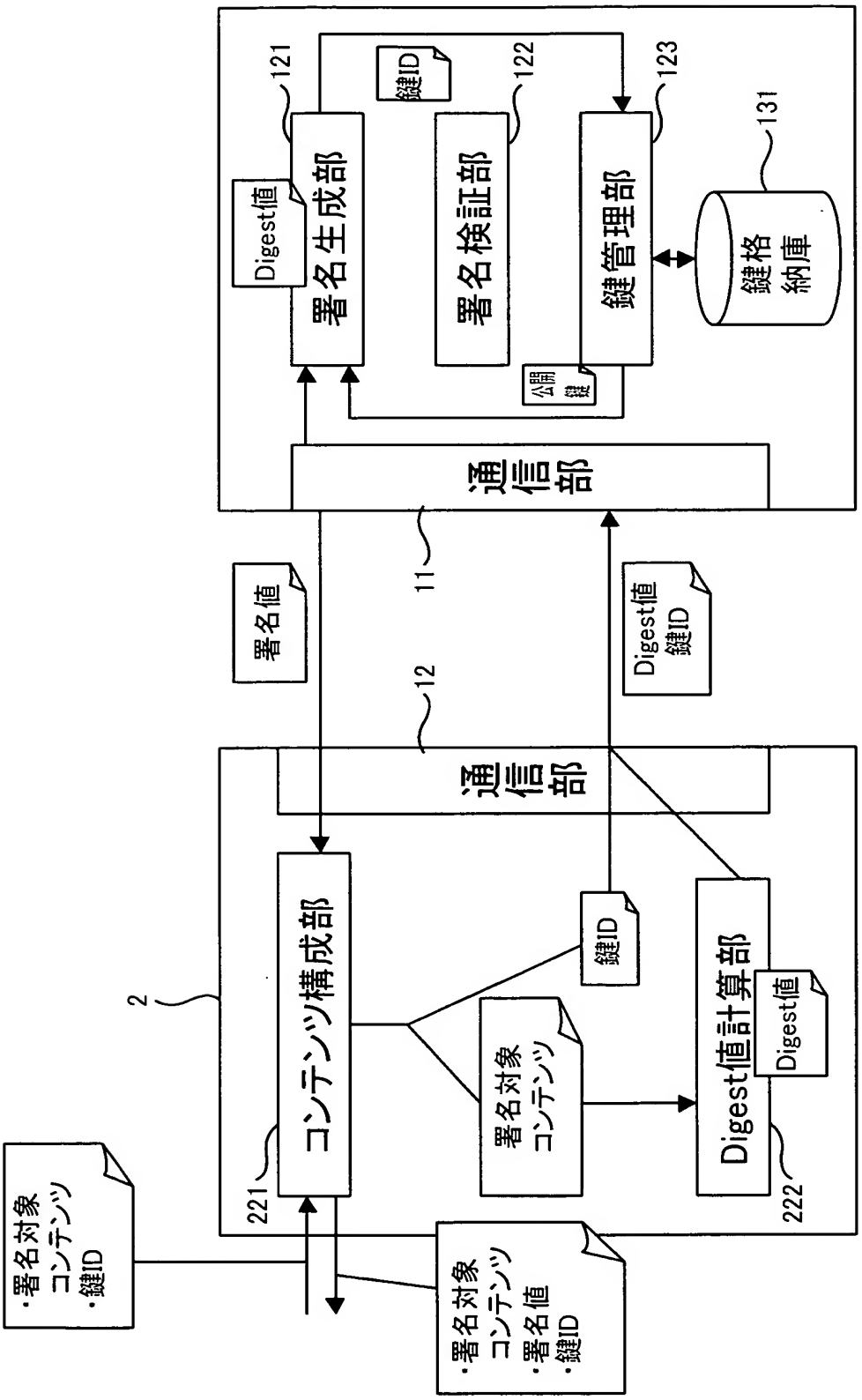
【図３】



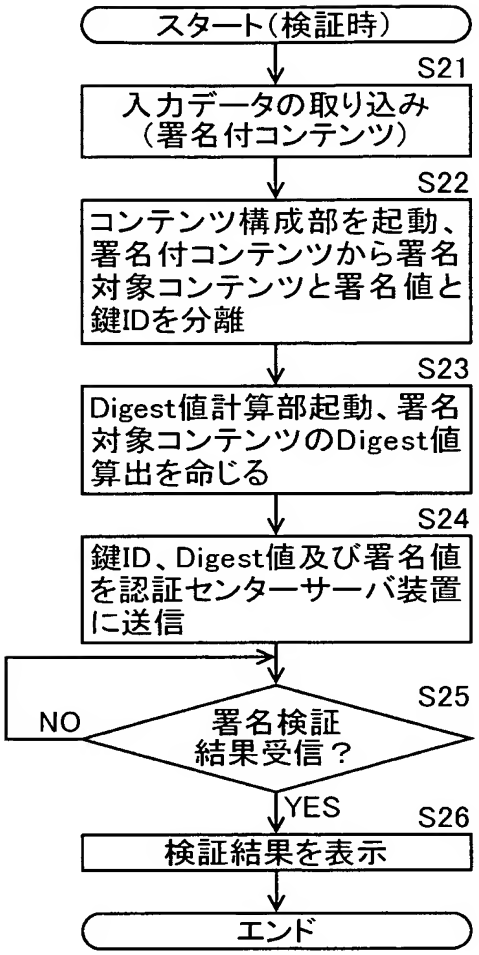
【図４】


鍵ID&Digest値受信によりスタート(署名時)
S11
鍵管理部を起動、鍵IDに対応する秘密鍵の検索を命じる
S12
署名生成部が、ダイジェスト値を暗号化して署名値を生成する
S13
署名値をユーザ端末へ送信
エンド

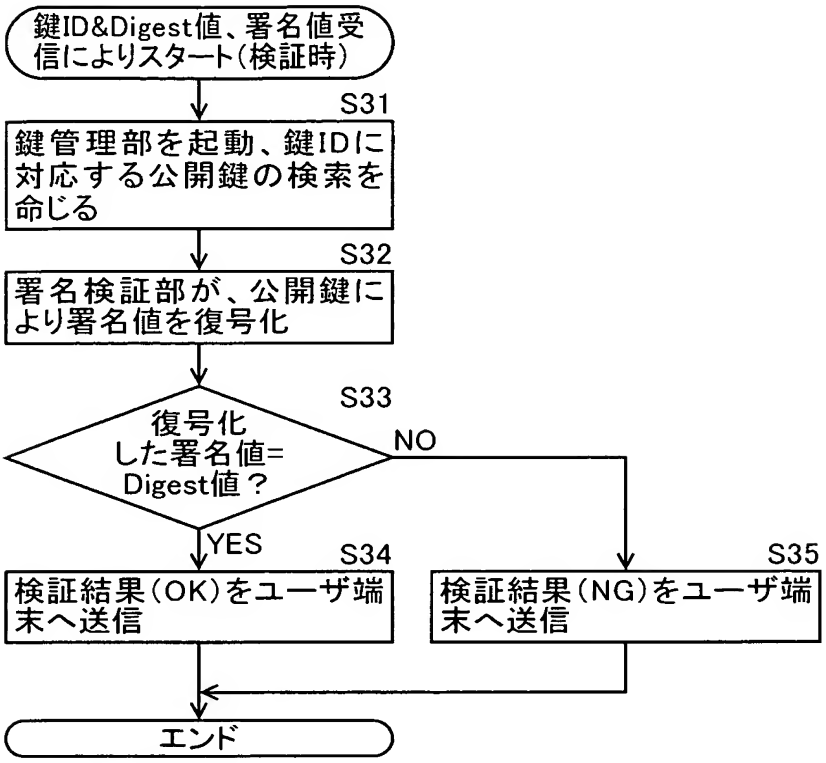
【図５】


121
122
123
131
鍵ID
Digest値
署名生成部
署名検証部
鍵管理部
鍵格納庫
公開鍵
通信部
11
署名値
Digest値
鍵ID
12
通信部
2
コンテンツ構成部
鍵ID
署名対象コンテンツ
Digest値計算部
Digest値
221
222
・署名対象コンテンツ
・鍵ID
・署名対象コンテンツ
・署名値
・鍵ID

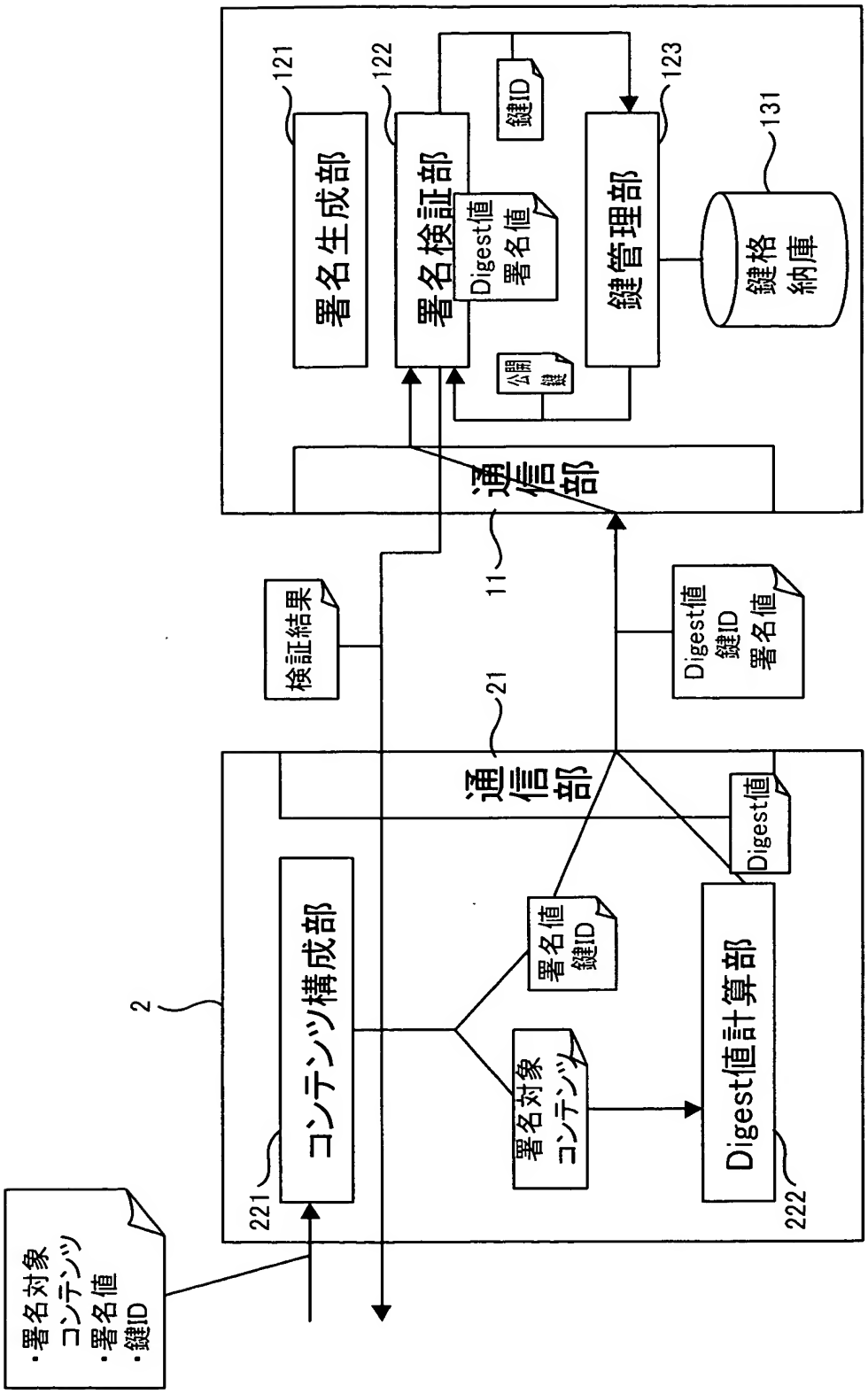
【図６】


スタート（検証時）
S21
入力データの取り込み（署名付コンテンツ）
S22
コンテンツ構成部を起動、署名付コンテンツから署名対象コンテンツと署名値と鍵IDを分離
S23
Digest値計算部起動、署名対象コンテンツのDigest値算出を命じる
S24
鍵ID、Digest値及び署名値を認証センターサーバ装置に送信
S25
署名検証結果受信？
NO
YES
S26
検証結果を表示
エンド

【図７】


鍵ID&Digest値、署名値受信によりスタート(検証時)
S31
鍵管理部を起動、鍵IDに対応する公開鍵の検索を命じる
S32
署名検証部が、公開鍵により署名値を復号化
S33
復号化した署名値=Digest値？
NO
YES
S34
検証結果(OK)をユーザ端末へ送信
S35
検証結果(NG)をユーザ端末へ送信
エンド

【図８】


・署名対象コンテンツ
・署名値
・鍵ID
2
221
コンテンツ構成部
署名対象コンテンツ
署名値
鍵ID
通信部
21
Digest値
Digest値計算部
222
検証結果
11
通信部
Digest値
鍵ID
署名値
121
署名生成部
122
署名検証部
Digest値
署名値
鍵ID
公開鍵
123
鍵管理部
131
鍵格納庫

【書類名】　要約書

【要約】

【目的】　署名対象電子情報そのものをサーバ装置において暗号化又は復号化することなく電子署名の作成及び検証を行うことができる電子署名作成方法及び電子署名検証方法を、提供する。

【構成】

電子情報の発行元利用者の端末２は、コンテンツのDigest値を算出し、このDigest値及び発行元利用者の鍵ＩＤを認証センターサーバ装置１へ送信する。認証センターサーバ装置１は、鍵ＩＤに対応した秘密鍵を鍵格納庫１３１から検索し、この秘密鍵によってDigest値を暗号化することによって署名値を生成し、署名値を上記利用者端末２へ応答する。利用者端末２は、受信した署名値及び鍵ＩＤを署名対象電子情報に添付することによって電子署名付きコンテンツを構成して、相手方へ発行する。相手方利用者の端末２は、電子署名付きコンテンツ中のコンテンツのDigest値を算出し、このDigest値，署名値及び添付鍵ＩＤを認証センターサーバ装置１へ送信する。認証センターサーバ装置１は、鍵ＩＤに対応した公開鍵を鍵格納庫１３１から検索し、この公開鍵によって署名値を復号化し、その復号結果がDigest値と一致するか否かを検証し、その検証結果を利用者端末２へ応答する。

【選択図】　図１

認定・付加情報

特許出願の番号	特願２００３－０９２２８０
受付番号	５０３００５２０６９０
書類名	特許願
担当官	第七担当上席　　００９６
作成日	平成１５年　４月　７日

＜認定情報・付加情報＞

【提出日】　平成15年 3月28日

次頁無

特願２００３－０９２２８０

出　願　人　履　歴　情　報

識別番号　　［０００００５２２３］

１．変更年月日　　１９９６年　３月２６日
［変更理由］　　住所変更
住　所　　神奈川県川崎市中原区上小田中４丁目１番１号
氏　名　　富士通株式会社